FYi
From the Information Policy Analysis Division

Summer 2005
VOLUME 4 ISSUE 4

Responding to Data Requests: Back to the Basics

By Corrine H. Thomson,
Guest Columnist
Kennedy & Graven, Chartered

Many people might assume that an article about responding to requests under the Minnesota Government Data Practices Act (the "MGDPA" or the "Act") would focus on data classification issues. After all, the first question many responsible authorities think of when a request is made is, "What is the data's classification?" There are, however, other issues to think about *before* you get to the question of the data's classification. This article focuses on the fundamentals of reviewing a data request and preparing your response.

Reviewing the Request

It sounds trite, but the appropriate *response* to a data practices request will always depend upon what is *requested*. Your response should begin with careful review of the request. You should ask yourself a number of questions. Is the request a request for data or merely a question? An entity is only required to respond to requests either to have access to or to acquire copies of government data as those data exist in a particular format (*Advisory Opinion No. 02-039*). If it is only a question, you may still respond, as a customer service issue, but you don't need to worry about complying with requirements of the Act, including timelines.

You should determine whether the information requested is "government data." That term has a broad reach (*See Minn. Stat. § 13.02, subd. 7*). The term does not include, however, information that does not exist in a physical form, such as mental impressions of a public officer (*Keezer v. Spickard*, 493 N.W.2d 614 (Minn. Ct. App. 1992)). Nor does it include "personal data" – data created by a government employee's authorized personal use of government equipment, such as a computer or voicemail system (*Advisory Opinion No. 01-075* [but see *Advisory Opinion No. 02-049* for a limitation on the exception for "personal data"]). An entity is neither required to nor prohibited from providing access to personal data.

Does the requested data even exist? The Act does not require entities to create new data or organize or reconfigure existing data into a different format or compilation. An entity may refuse to create data or, if it elects to create the data, it may impose any charge that is acceptable to both the entity and the requestor. (*See Advisory Opinion No. 96-007*). If the request requires creation of data, the entity should clarify that with the requestor before proceeding (*Advisory Opinion No. 99-034*).

It is critical that you understand what is being requested. Lack of clarity in requests (and in responses) is a recurring theme in advisory opinions issued by the Commissioner of Administration. If you need clarification in order to respond, seek it promptly (*Advisory Opinion No. 04-003*). Avoid making "assumptions" about what a requestor is really seeking (*Advisory Opinion No. 03-038*). You may require the request in writing, not to provide a barrier to access, but to assure clarity and to avoid

Back to the Basics
Please see Page 3

Information Policy Analysis Division

Minnesota Department of Administration

Legislative Update 2005

This is the first article documenting changes enacted by the Legislature in 2005. The focus of this article is on the Omnibus Data Practices bill; other legislation will be summarized in the fall edition of *FYi*.

As is its custom, the Legislature has combined many bills into an omnibus data practices bill for 2005. For those not familiar with the conference committee process, the purpose is to resolve the differences between the House and Senate bills and reach agreement on language that both bodies can enact. As with most conference committees, there was some proposed language about which the members of the conference committee could not agree.

In 2005, the language where there was no agreement was: (a) increases in the penalty amounts in section 13.08; (b) changes to language governing claims data held by service cooperatives; (c) classification of employee mediation data at the Department of Transportation; (d) authority for the Department of Finance to access tax return data at the Department of Revenue; (e) language controlling the use of data obtained by scanning a driver's license or similar identification card; and (f) a requirement for the Department of Public Safety to contract for an audit of the motor vehicle tab renewal website.

HF 225 (Chapter 163)
Omnibus Data Practices Bill
Signed June 3, 2005

The text of the bill is available on the Internet at www.revisor.leg.state.mn.us/bin/bldbill.php?bill=H0225.3&session=ls84.

Section 1 amends section 3.978, subdivision 2 to make it clear that the Legislative Auditor has access to any data regardless of its classification.

Section 2 provides a data classification for data held by the State Board of Investment (SBI). According to testimony provided during the committee process, those companies and services providing investment vehicles to the SBI will not do business with Minnesota or provide certain data without the ability to have the data protected from public disclosure. NOTE: This language will *not* appear in Minnesota Statutes as similar language was enacted in Chapter 156, Article 2, Section 7. Chapter 156 was signed later than Chapter 163 and so the rules of statutory interpretation require that the language enacted later is what is included in the statutes. Also, the language in Chapter 156 is effective June 4, 2005.

Sections 3-20 and 22-31 all contain the same change: replacing "state agency, political subdivision or statewide system" with the defined phrase "government entity" (which is defined as "state agency, political subdivision or statewide system") or changing references to "agency" to "entity." These changes are made in sections 13.01 through 13.09.

In addition, **Section 8** contains a change to section 13.03, subdivision 3 (c) that will set a specific charge for black-and-white, legal- or letter-sized paper copies of *public* data in certain circumstances. First, the request must result in 100 or fewer pages. Second, the responsible authority must decide to charge a fee for these types of copies. Third, the cost can be no more than 25 cents for each page. Testimony during the committee process indicated that a "page" is one side of a piece of paper, so a two-sided copy would have a maximum cost of 50 cents.

Section 21 adds a new responsibility for state agencies that will be found in section 13.055. Specifically, if a state agency holds private or confidential data on individuals and there is a breach of the security of the data (defined term), the state agency is required to notify each individual of the breach. The language is patterned on language from California that was used to notify individuals that ChoicePoint and others had suffered a breach

Legislative Update 2005
Please see Page 4

Back to the Basics: Responding to Requests

Continued from the front page

misunderstandings (*See Advisory Opinion No. 01-007*).

Was the request made to the correct person? Under the MGDPA, requests for access to data must be made to the responsible authority or his/her designees (*Minn. Stat. § 13.03, subd. 3*). If the request is made to someone else, and the entity intends to rely upon that requirement, then the entity must inform the requestor and direct the requestor to the responsible authority at the time the request is made (*Advisory Opinion No. 96-051*).

You should carefully consider *who* is making the request. An entity cannot require a requestor to identify him/herself or justify a request for access to public data. However, a person may be asked to provide identifying or clarifying information for the sole purpose of facilitating access to the data (*Minn. Stat. § 13.05, subd. 12*). Obviously, you must determine the identity of anyone seeking access to data classified as not public, to prevent unauthorized access.

In determining who is making the request, the first focus should be on whether the requestor *is* the subject of the data or *is not* the subject of the data. The answer to that question affects both the deadline for providing a response and the charges that can be imposed. After the issue of "data subject" vs. "member of the public" has been determined, the data classification can be determined and, if the classification is "not public," *then* the focus should be on the identity of the requestor.

The determination of who is the subject of the data must be made on a case-by-case basis, by reviewing each document requested (*Advisory Opinion No. 02-019*). For guidance in making that determination, look to Minn. Stat. § 13.02, subd. 5. That subdivision defines "data on individuals" as data in which any individual can be identified as a subject of the data "unless the appearance of the name or other identifying data can be *clearly demonstrated* to be only incidental to the data *and* the data are not accessed by the name or other identifying data of the individual (*emphasis added*)."

You should also consider how the request is framed. Access to data may be determined by how it is requested. For example, in *Advisory Opinion No. 95-005*, a reporter made requests to a school about whether the school had received the complaint of alleged sexual harassment of a student, the status of the complaint and a copy of the notice of claim. All of that information would be public if it had been requested in that manner. But the school district responded that the reporter had not asked about a complaint of sexual harassment of "a" student, but instead had asked about a complaint made by a particular student, whom the reporter named. The identity of the student was private, and under the circumstances the disclosure of the information would have disclosed information about that student. Therefore, the school's refusal to provide the information was an appropriate response. See *Advisory Opinion Nos. 00-020 and 02-048* for similar examples of how the nature of the request can determine the appropriate response. The framing of the question can also impact the determination of who the data subjects are (*Advisory Opinion No. 02-019*).

Back to the basics on responses

Always respond. Failure to respond is never appropriate (*Advisory Opinion No. 97-020*). The potential options for a response are also fairly limited. They include:

(1) The data you have requested is available and ready for inspection or the copies you requested are available.

(2) The data you requested does not exist (*Advisory Opinion No. 97-020*).

(3) The data that you requested is not available for inspection or copying, and the applicable statutory section that prevents access is Minn. Stat. § 13.03, subd. 3(f) *(Advisory Opinion No. 98-006).* An entity must inform the requestor of the existence of data that has been requested but to which access is denied (*Advisory Opinion Nos. 94-003, 97-008*).

(4) In order to properly respond to your data request, we need clarification of [describe what clarification is needed].

(5) The information you requested is not government data because [explain why not – possible options being that it is only a mental impression (but then it is not data at all) or it is personal data (see *Advisory Opinion No. 01-075*). In such circumstances, further response is at the option of the entity and outside the scope of the MGDPA.]

BE CLEAR in your response (*Advisory Opinion No. 02-017*). The response should be specific to the particular request and should respond to every element of the request (*Advisory Opinion No. 00-014*).

Conclusion

Data practices compliance is not simple. One way to simplify the complexity, though, is to break it down into manageable pieces. When you receive a request, review it carefully. Always respond to every element of the request and respond in a timely fashion.

Legislative Update 2005

Continued from Page 2

in their security. Similar language in HF 2121/Chapter 167 will govern the private sector and requires government entities to do a comprehensive security assessment.

Section 32 moves existing language about education records of children with disabilities from section 13.04, subdivision 5 to section 13.32 with other language concerning education data.

Sections 33, 34, 42 and 51 all relate to situations in which one government entity is responding to a request for bid or proposal from another government entity. Under current law, data in a response would be public and put a government entity at a disadvantage vis-à-vis private sector bidders or responders. These changes move language from section 13.37 to section 13.591 and delete language specific to state agencies regarding responses.

Section 35 amends section 13.37 to authorize the sharing of security information when to do so would "aid public health, promote public safety, or assist law enforcement" and the responsible authority for the data has consulted with appropriate public health, law enforcement and emergency management officials.

Section 36 brings uniformity to the classification of data about those who are found to have maltreated a vulnerable adult. The new language, to be coded in section 13.3805, also defines what makes an individual a "substantiated perpetrator" of abuse and makes the data that identify these individuals public.

Sections 37, 38, 39 and 43 all relate to data about applicants for election or appointment to a public body. Sections 37, 38 and 39 remove language relating to applicants for appointment from section 13.43 and new language is added to section 13.601 in section 43 to specify that certain data about applicants are public.

Section 40 amends section 13.46, subdivision 4, addresses two issues regarding licensing. The first makes public more data about licensees. Specifically, data about training and education in childcare and child development and the number of serious injuries or deaths will be public. The second makes public data that identify a "substantiated perpetrator."

Section 41 classifies as protected nonpublic data that are created or maintained by a government entitiy as part of the evaluation of a bid or proposal. The data become public upon completion of the selection process (in the case of a bid) or completion of the evaluation process (in the case of a proposal). In addition, there is new language that authorizes state agencies to share protected nonpublic data with employees from other state agencies as part of the selection or evaluation process.

Section 44 provides a cross-reference to the new language in section 2 relating to the State Board of Investment.

Section 45 classifies data at the Board of Animal Health about animals and the locations where they are kept. The classifications are private or nonpublic and relate to data about the outbreak of diseases. There is also authority for the Board to share the data in certain circumstances.

Sections 46, 47 and 48 classify data at the Department of Transportation. The first two sections add subdivisions to section 13.72 and classify data used in the design-build process. As with data in section 13.591, the classified data become public at specific, defined points in the process. Section 48 classifies data about the use of toll facilities as well as financial information used to pay the tolls.

Section 49 amends the list of law enforcement entities that are subject to section 13.82. In the 2004 session, the Division of Insurance Fraud at the Department of Commerce was specifically named. The 2005 change removes the division limitation and makes the section applicable to any law enforcement function at the Department. This section was effective June 4, 2005.

Section 50 amends section 13.82, subdivision 16 to make it clear that when a law enforcement agency makes data public, it must separate the not public (not just the confidential) data from the public data. This section was effective June 4, 2005.

Legislative Update 2005

Please see Page 6

Opinion Highlights

The following are highlights of recent advisory opinions by the Commissioner of Administration. All Commissioner's opinions are available on the IPAD web site at www.ipad.state.mn.us.

05-018: The *Saint Paul Pioneer Press* asked whether the City of Saint Paul had complied with Minnesota Statutes, Chapter 13, in responding to a data request regarding a former head of one of the City's departments. The Commissioner concluded that because a final disposition had not occurred, only the existence and status of any complaint was public. In addition, the Commissioner reiterated the position taken in previous advisory opinions that section 13.43, subdivision 2(e), does not apply to local government officials.

05-019: The Winona Housing and Redevelopment Authority (HRA) asked whether, pursuant to Chapter 13, a complainant is entitled to gain access to certain data s/he provided relating to the complaint. The Commissioner opined that the HRA would not be in compliance if it provides a complainant access to data that consist of an investigator's notes and interview summaries, because those data are private personnel data about employees other than the complainant, and are not a "statement provided by the complainant" for purposes of section 13.43, subdivision 2(d).

05-020: An individual asked whether Resource Training and Solutions (RTS) was in compliance with Chapter 13 when RTS required him to inspect data at the offices of its attorney, some 60 miles away. The Commissioner opined that such a response was not appropriate given the language in section 13.03, subdivision 3, providing that individuals be permitted to inspect and copy public government data at reasonable times and places.

05-021: Independent School District 196, Rosemount-Apple Valley-Eagan, asked (1) whether section 13.34 applies to written K-12 classroom tests and quizzes that count toward a student's grade and (2) whether the District would be in compliance with Chapter 13 and federal law if it declined to provide students (and the parents of minor students) with copies of their completed tests and quizzes, but provided the students with access to their completed examinations by allowing them to inspect and review completed tests and quizzes in school. The Commissioner concluded that the answer to both questions is yes.

05-022: Independent School District 701, Hibbing, asked whether it would be in compliance with Chapter 13 if it released to the District's Pupil Support Assistants (as a group), certain identifying data about students with disabilities. Upon reviewing state and federal law, the Commissioner opined that the District would not be in compliance if it released the data to Pupil Support Assistants whose work assignments do not require that they gain access and who have no legitimate educational interest in the data.

05-023: The Washington County Housing and Redevelopment Authority asked about the classification of certain data relating to properties it owns: street addresses of rental property occupied by recipients of rental assistance benefits. The Commissioner, relying on section 13.462, opined that the data are private.

Information Policy Analysis Division

Questions or comments?

Contact the Information Policy Analysis Division at 201 Administration Building, 50 Sherburne Avenue, St. Paul, MN, 55155; phone 800.657.3721 or 651.296.6733; fax 651.205.4219; email info.ipad@state.mn.us.

Staff: Laurie Beyer-Kropuenske, *Director,* Katie Engler, Janet Hey, Brooke Manley, Linda Miller and Catherine Scott.

This document can be made available in alternative formats, such as large print, Braille or audiotape by calling 651.296.6733.

For TTY communication, contact the Minnesota Relay Service at 800.627.3529 and ask them to place a call to 651.296.6733.

Legislative Update 2005

Continued from Page 4

Sections 52-57 authorize certain boards at the Department of Employment and Economic Development (DEED) to conduct meetings using telephone conference calls. In each instance, certain conditions must be met before and during the telephone conference call.

Sections 58 and 78 direct the Department of Public Safety to treat and disclose motor vehicle registration and driver's license data as provided in the federal Driver's Privacy Protection Act, 18 United States Code section 2721. State provisions are also changed so that motor vehicle and driver's license data are disclosed only after the individual "opts in" to the disclosure, as is required by the federal law. When the personal safety of an individual requires that data be classified as private, application must be made to the Commissioner of Public Safety for that treatment.

Sections 59-73 and 75-77 contain technical corrections sought by the Department of Public Safety and all relate to the operation of motor vehicles and drivers.

Section 74 authorizes the Department of Public Safety to release motor vehicle and driver's license data to individuals involved in an accident where law enforcement does not complete an accident report.

Section 79 makes the state taxpayer identifying number of a business public data at the Department of Revenue.

Section 80 outlines who can access business tax returns on behalf of a business.

Section 81 describes how data in the new Comprehensive Incident-Based Reporting System (CIBRS) will be classified and disclosed. CIBRS is a statewide system that will be operated by the Bureau of Criminal Apprehension on behalf of law enforcement agencies statewide. Data in CIBRS will be classified as confidential and become private on the occurrence of specifically described circumstances.

Section 82 prohibits the Department of Public Safety from establishing a subscription service (defined term) for law enforcement personnel without prior legislative authorization.

Sections 83 and 84 state that wireless telephone directories can only be established if the customer provides specific authorization for his/her wireless number to be included in the directory. This section was effective June 4, 2005.

Section 85 adds a section to chapter 325E and prohibits any person or entity from using or requiring the disclosure of Social Security numbers in certain circumstances. The provisions apply to the private sector and appear to apply to Minnesota state colleges and universities and the University of Minnesota. They do not apply to other government entities.

Section 86 directs the Commissioner of Public Safety to submit two reports. The first relates to the CIBRS database and the second is about the advisability of prohibiting the possession or use of devices to falsify results of drug and alcohol testing.

Section 87 directs the Commissioner of Administration to submit a report on how the State handles genetic information and how release or nonrelease affects the privacy of relatives of the individuals about whom the data are maintained.

Section 88 is an instruction to the Revisor regarding statutes related to motor vehicles.

Section 89 contains repealers. Section 13.04, subdivision 5 is the language that was moved to section 13.32 by section 32 (above). Sections 169.09, subdivision 10 and 170.55 are about substituted service of process on drivers and new language is found in sections 59-73 and 75-77.